Isogeny-basd cryptography III

Isogenies

Tanja Lange
(with lots of slides by Lorenz Panny)

Eindhoven University of Technology

SAC – Post-quantum cryptography

Isogenies

An isogeny of elliptic curves is a non-zero map $E \to E'$

- given by rational functions
- that is a group homomorphism.

The degree of a separable isogeny is the size of its kernel.

Isogenies

An isogeny of elliptic curves is a non-zero map $E \to E'$

- given by rational functions
- that is a group homomorphism.

The degree of a separable isogeny is the size of its kernel.

Example #1: For each $m \neq 0$, the multiplication-by-m map

$$[m]\colon E \to E$$

is an isogeny from E to itself.

If $m \neq 0$ in the base field, its kernel is

$$E[m] \;\cong\; \mathbb{Z}/m \times \mathbb{Z}/m.$$

Thus $[m]$ is a degree-m^2 isogeny.

Isogenies

An isogeny of elliptic curves is a non-zero map $E \to E'$

- given by rational functions
- that is a group homomorphism.

The degree of a separable isogeny is the size of its kernel.

Example #2: For any a and b, the map $\iota \colon (x, y) \mapsto (-x, \sqrt{-1} \cdot y)$ defines a degree-1 isogeny of the elliptic curves

$$\{y^2 = x^3 + ax + b\} \longrightarrow \{y^2 = x^3 + ax - b\}\,.$$

It is an isomorphism; its kernel is $\{\infty\}$.

Isogenies

An isogeny of elliptic curves is a non-zero map $E \to E'$

- given by rational functions
- that is a group homomorphism.

The degree of a separable isogeny is the size of its kernel.

Example #3:

$$(x, y) \mapsto \left(\frac{x^3-4x^2+30x-12}{(x-2)^2}, \frac{x^3-6x^2-14x+35}{(x-2)^3} \cdot y \right)$$

defines a degree-3 isogeny of the elliptic curves

$$\{y^2 = x^3 + x\} \;\longrightarrow\; \{y^2 = x^3 - 3x + 3\}$$

over $\mathbb{F}_{71}$. Its kernel is $\{(2,9),(2,-9),\infty\}$.

Topic of this lecture

- Isogenies are well-behaved maps between elliptic curves.

Topic of this lecture

- Isogenies are well-behaved maps between elliptic curves.

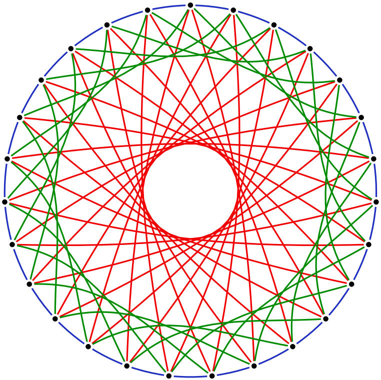
$\rightsquigarrow$ Isogeny graph: Nodes are curves, edges are isogenies.

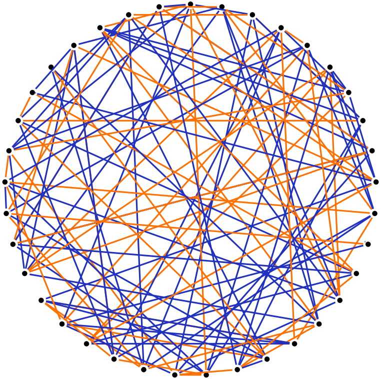
(We usually care about subgraphs with certain properties.)

- Isogenies give rise to post-quantum Diffie–Hellman (and more!)

The beauty and the beast

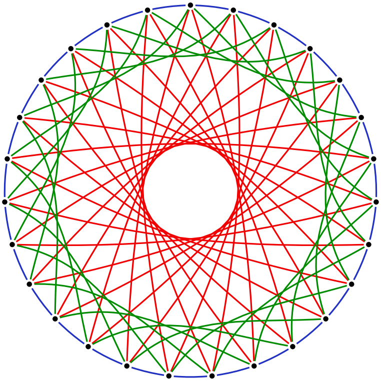
Components of well-chosen isogeny graphs look like this:

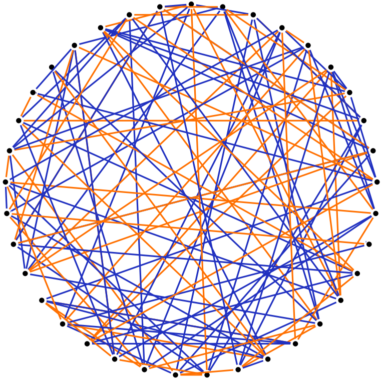




The beauty and the beast

Components of well-chosen isogeny graphs look like this:

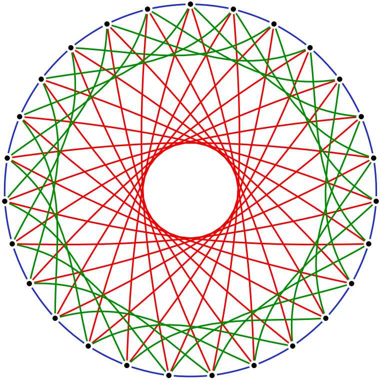


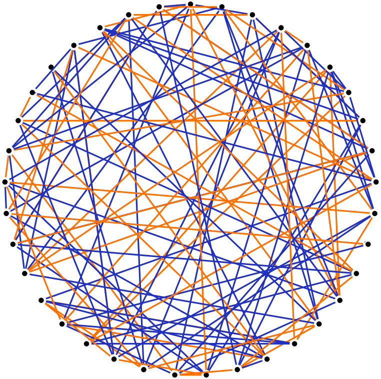


Which of these is good for crypto?

The beauty and the beast

Components of well-chosen isogeny graphs look like this:

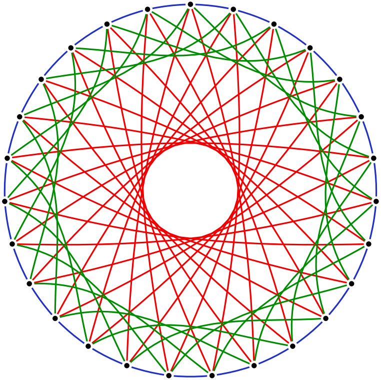




Which of these is good for crypto? **Both.**

The beauty and the beast

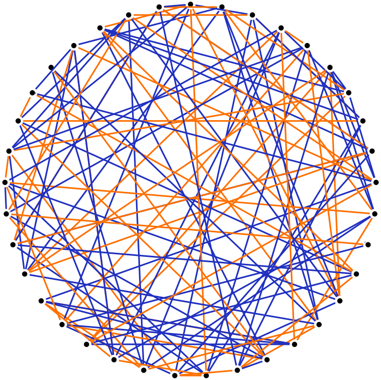
At this time, there are two distinct families of systems:



$q = p$

CSIDH [ˈsiːˌsaɪd]

https://csidh.isogeny.org



$q = p^2$

SIDH

https://sike.org

CSIDH [ˈsiːˌsaɪd]

(Castryck, Lange, Martindale, Panny, Renes; 2018)

Why CSIDH?

- Closest thing we have in PQC to normal DH key exchange: Keys can be reused, blinded; no difference between initiator &responder.
- Public keys are represented by some $A \in \mathbb{F}_p$; p fixed prime.
- Alice computes and distributes her public key A.
  Bob computes and distributes his public key B.
- Alice and Bob do computations on each other's public keys to obtain shared secret.
- Fancy math: computations start on some elliptic curve $E_A : y^2 = x^3 + Ax^2 + x$, use isogenies to move to a different curve.
- Computations need arithmetic (add, mult, div) modulo p and elliptic-curve computations.

CSIDH in one slide

CSIDH in one slide

- Choose some small odd primes $\ell_1, ..., \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.

CSIDH in one slide

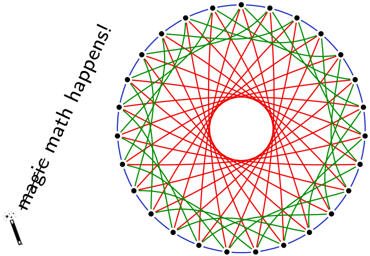
- Choose some small odd primes $\ell_1, ..., \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p+1$ points$\}$.

CSIDH in one slide

- Choose some small odd primes $\ell_1, ..., \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p+1$ points$\}$.
- Look at the ℓ_i-isogenies defined over $\mathbb{F}_p$ within X.

CSIDH in one slide

- Choose some small odd primes $\ell_1, \ldots, \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p+1$ points$\}$.
- Look at the ℓ_i-isogenies defined over $\mathbb{F}_p$ within X.



$p = 419$

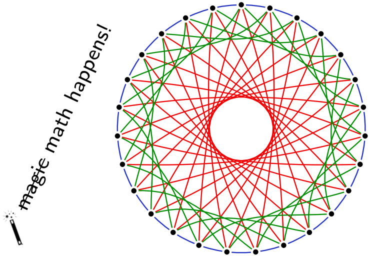
$\ell_1 = 3$

$\ell_2 = 5$

$\ell_3 = 7$

CSIDH in one slide

- Choose some small odd primes $\ell_1, \ldots, \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p+1$ points$\}$.
- Look at the ℓ_i-isogenies defined over $\mathbb{F}_p$ within X.



$p = 419$

$\ell_1 = 3$

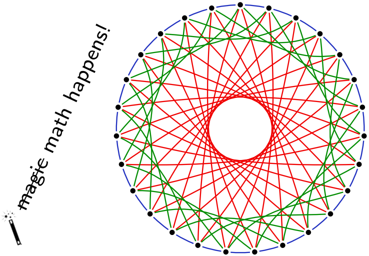
$\ell_2 = 5$

$\ell_3 = 7$

- Walking "left" and "right" on any ℓ_i-subgraph is efficient.

CSIDH in one slide

- Choose some small odd primes $\ell_1, \ldots, \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p+1$ points$\}$.
- Look at the ℓ_i-isogenies defined over $\mathbb{F}_p$ within X.



$p = 419$
$\ell_1 = 3$
$\ell_2 = 5$
$\ell_3 = 7$

- Walking "left" and "right" on any ℓ_i-subgraph is efficient.
- We can represent $E \in X$ as a single coefficient $A \in \mathbb{F}_p$.

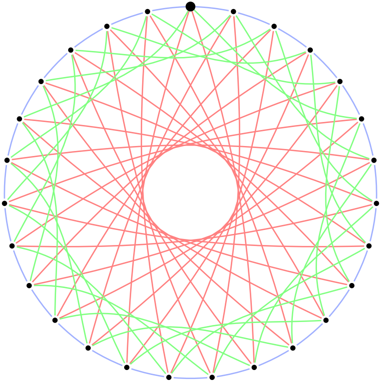
CSIDH key exchange

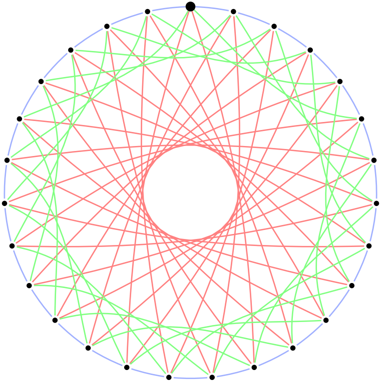
Alice

$[+, +, -, -]$

Bob

$[-, +, -, -]$

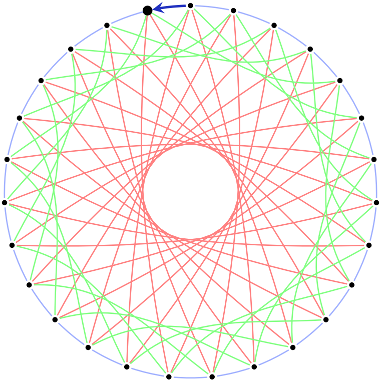




CSIDH key exchange

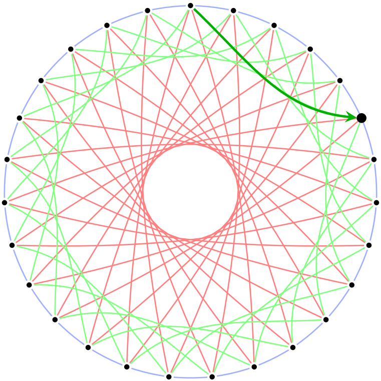
Alice

$[\underset{\uparrow}{+}, +, -, -]$



Bob

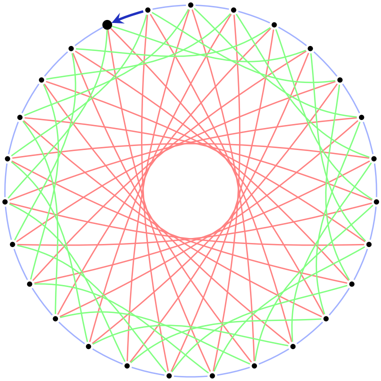
$[\underset{\uparrow}{-}, +, -, -]$



CSIDH key exchange

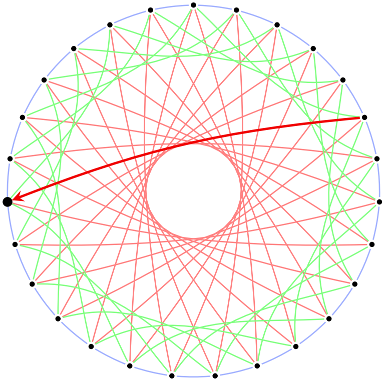
Alice

$[+, \underset{\uparrow}{+}, -, -]$



Bob

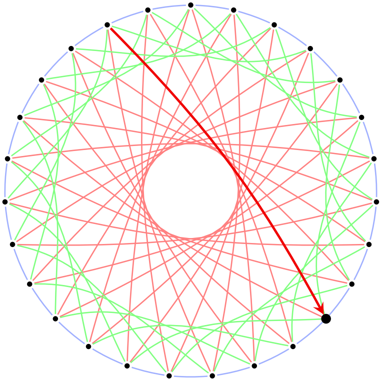
$[-, \underset{\uparrow}{+}, -, -]$



CSIDH key exchange

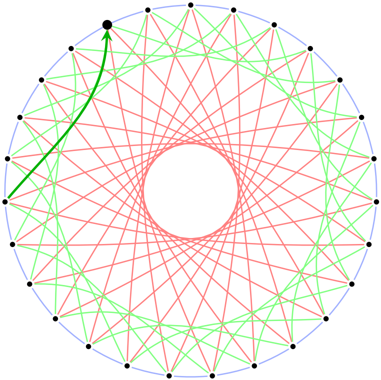
Alice

$[+,+,\underset{\uparrow}{-},-]$



Bob

$[-,+,\underset{\uparrow}{-},-]$



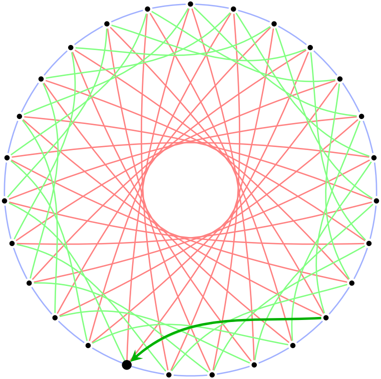
CSIDH key exchange

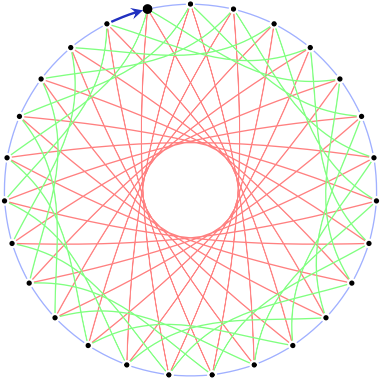
Alice

$[\textcolor{blue}{+}, \textcolor{blue}{+}, \textcolor{red}{-}, \underset{\uparrow}{\textcolor{green}{-}}]$

Bob

$[\textcolor{green}{-}, \textcolor{red}{+}, \textcolor{green}{-}, \underset{\uparrow}{\textcolor{blue}{-}}]$





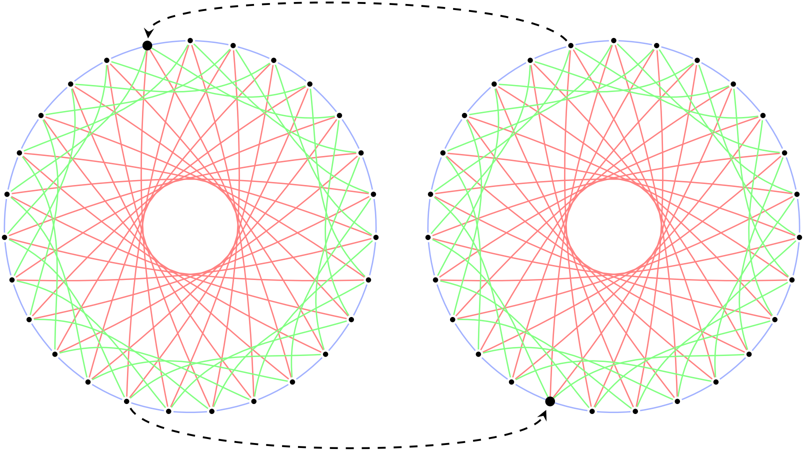
CSIDH key exchange

Alice

$[+, +, -, -]$

Bob

$[-, +, -, -]$

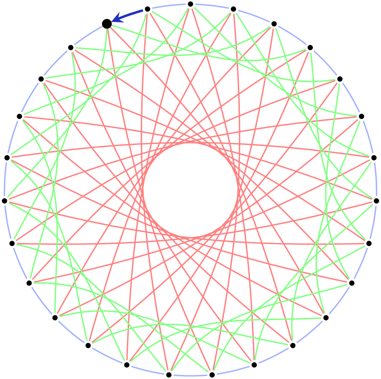


CSIDH key exchange

Alice

[+, +, −, −]

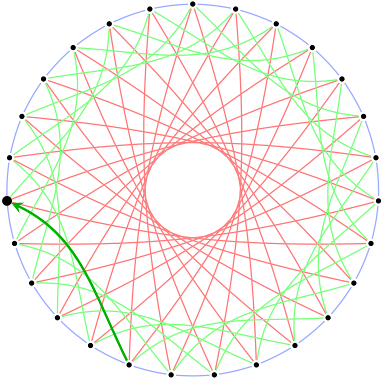
↑



Bob

[−, +, −, −]

↑



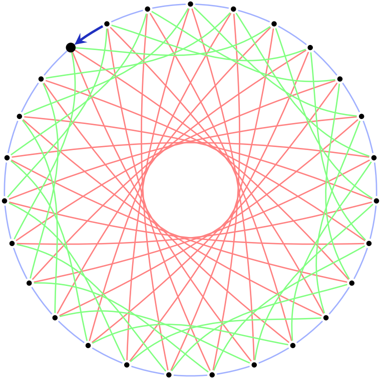
CSIDH key exchange

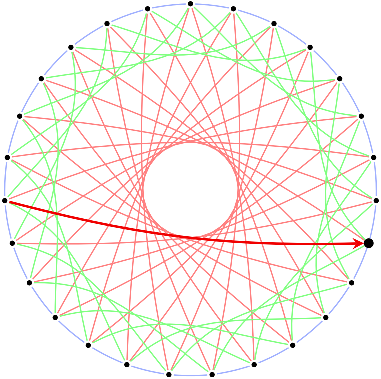
Alice

[**+**, **+**, **−**, **−**]
↑

Bob

[**−**, **+**, **−**, **−**]
↑





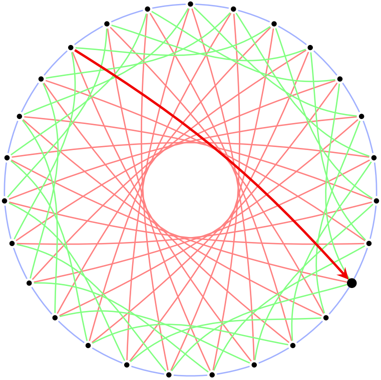
CSIDH key exchange

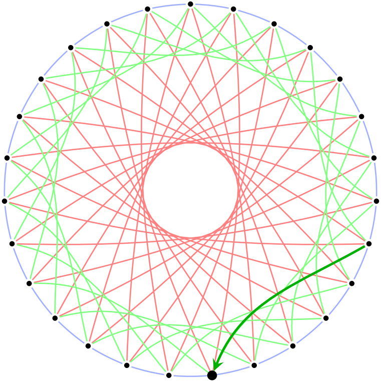
Alice

$[+, +, \underset{\uparrow}{-}, -]$

Bob

$[-, +, \underset{\uparrow}{-}, -]$





CSIDH key exchange

Alice

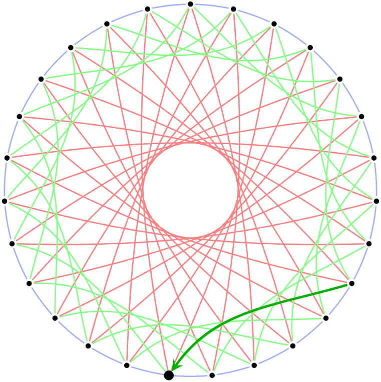
$[+, +, -, -]$

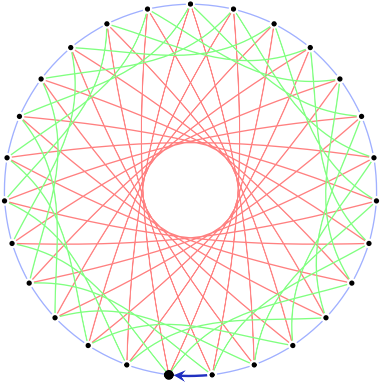
↑

Bob

$[-, +, -, -]$

↑

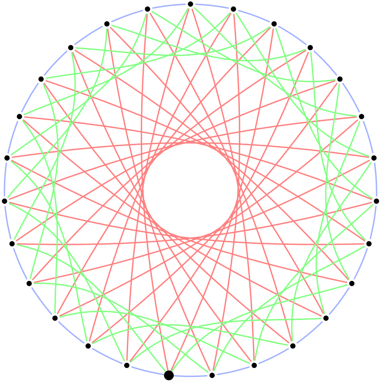




CSIDH key exchange

Alice

[+, +, −, −]



Bob

[−, +, −, −]